REMARKS/ARGUMENTS

This Amendment is in response to the Office Action dated January 27, 2004. Claims 1-30 are pending. Claims 1-30 have been canceled, and Applicant has added claims 31-60. Accordingly, claims 31-60 are pending in the present application.

New Claims

Applicant has added claims 31-60, which clarify the present invention. Support for the new claims is found throughout the Specification, for instance starting at page 4, line 17 to page 8, line 7. Applicant respectfully submits that no new matter has been presented.

35 U.S.C. §101 Rejections

The Examiner rejected claims 1, 11 and 21 under 35 U.S.C. §101 as being unpatentable for failing to apply, involve, use or advance the technological arts, and for failing to produce a useful, concrete, and tangible result. Applicant respectfully submits that the new claims satisfy the requirements under 35 U.S.C. §101.

35 U.S.C. §112 Rejections

The Examiner rejected claims 1, 11 and 21 under 35 U.S.C. §112 as being indefinite because the term "a portion of ..." was a relative term. Applicant respectfully disagrees.

The MPEP indicates that the term "*substantial* portion" can render a claim indefinite if the specification lacks some standard for measuring the degree intended (MPEP 2173.05(c)(F)). Nevertheless the term "*substantial portion*" is distinct from the term "*a portion.*" According to the dictionary, a "portion" is clearly defined as "a part or share of something larger." (Cambridge Dictionary, The American Heritage ® Dictionary of the English Language, Fourth Edition 2000).

A "substantial" portion is understandably vague in and of itself because the term "substantial" is a relative term.

In claims 36, 46 and 56, "a first portion" of a new encryption key is stored in the first system. In claims 39, 49 and 59, "the first value is a first portion of an encryption key and the second value is a whole encryption key." In the present invention, "a first portio" of an encryption key is just that, "a part or share of" the encryption key. In the Specification, the "first portion" of the encryption key is described as one-half of the encryption key (Spec., page 8, lines 11-12). Accordingly, Applicant respectfully submits that the term "a first portion" is not a relative term and does not render the claims indefinite under 35 U.S.C. §112, 2nd paragraph.

35 U.S.C. §102 Rejections

The Examiner rejected claims 1-5, 11-15 and 21-25 under 35 U.S.C. §102(b) as being anticipated by Kirsch (U.S. Patent No. 5,963,915) or Luckenbaugh et al (U.S. Patent No. 6,311,269). In so doing, the Examiner stated:

> **As per claims 1, 11, and 21, Kirsch and Luckenbaugh clearly disclose a method, system, and computer readable medium for conducting a transaction over a network, the network including a first system and a second system, the method, system, and program instructions comprising the steps of:**
> **(a) initiating a transaction session;**
> **(b) comparing a value of the first system with a value of the second system, wherein the value of the first system comprises a portion of an encryption key is associated with particular transaction session; and**
> **(c) continuing the transaction based on the comparison (See Kirsch abstract, figure 3 and associated text, column 3, lines 4-32, column 4, lines 48-64, and column 13, lines 15-51 and Luckenbaugh figures 2, 2B, 2C, 3 and 4 and associated text, column 3, lines 35-64, column 5, lines 14-64, column 7, lines 9-63, and column 8, lines 1-13 and lines 53-65. To clarify both Kirsch and Luckenbaugh systems establish communication between a client and a server to retrieve certain information from a server, once this communication is established the server checks the client for existence of a cookie if such cookie exist the server compares the cookie with existing cookies in the storage at the server. Once the cookie has been verified depending on the last transaction the cooki has been related to the transaction will continue.)**

Applicant submits that claims 31, 41 and 51 are analogous to canceled claims 1, 11 and 21. Applicant respectfully traverses.

The present invention is directed to a method and system for conducting a transaction between two computer systems over a network such as the Internet. Through the present invention, a customer purchasing a downloadable file over the Internet will not be charged more than once for a single file(s) if the connection to the Internet is somehow lost while the file(s) is being downloaded. According to the present invention, when the customer initiates a transaction via a computer system, e.g., by accessing a web site and selecting a file(s) for download, the server (that supports the web site) determines whether the transaction is a new transaction or one that was previously started and interrupted. The server makes this determination by comparing a value stored in the customer's computer system with a value stored in its system. (Spec. at page 4, line 17 to page 5, line 22). In a preferred embodiment, the value stored in the customer's computer system is a portion of an encryption key and the value stored in the server is a whole encryption key.

If the value stored in the customer's computer system does *not* match a part of the value stored in the server, the server concludes this is a new transaction and generates a new encryption key and replaces the value stored in the server with the new encryption key. This key is associated with the transaction and is used to encrypt the requested file(s). The server then sends a portion (e.g., one-half) of the key to be stored as the value in the customer's system. (Spec. at page 5, lines 5-15).

If, on the other hand, the values match, the server concludes that the transaction is one that was previously initiated but interrupted, and the server will resume the previously interrupted transaction. (Spec. at page 5, lines 19-22). Once the encrypted file(s) has been downloaded successfully and the customer has paid the fee, the remaining portion of encryption key is provided to the customer. (Spec. at page 6, lines 6-9).

The present invention, as recited in claim 31, provides:

31. A method for conducting a transaction between a first computer system and a second computer system, the method comprising the steps of:

(a) receiving in the second computer system a request from a user of the first computer system to download data from the second computer system;

(b) determining by the second computer system whether the request represents a new transaction or an incomplete transaction by comparing a first value stored in the first computer system with a second value stored in the second system; and

(c) if the request represents an incomplete transaction, completing the transaction,

wherein the user is not charged duplicate fees associated with starting a new transaction.

Claims 41 and 51 are system and computer product claims having scopes similar to that of claim 31.

Kirsch and Luckenbaugh are directed to methods for efficiently performing authenticated transactions between a client and a server over a network. In Kirsch, "[a] persistent predetermined coded identifier is established on the client browser corresponding to an account record stored by the merchant server." When the client wishes to purchase a product or service, the coded identifier is automatically transmitted to the merchant along with the client's selection, and the merchant "validates the predetermined coded identifier against the server stored account record." (Abstract; col. 4, lines 48-64).

Luckenbaugh is directed to implementing fine-grained access control to information stored in a server. In Luckenbaugh, a value stored in a cookie is mapped to the user's identity and credentials (access privilege) stored at the server. When the user submits a request for information from the server, the server analyzes the value in the cookie, if it exists, and based on that value returns data to the user. The cookie is referred to as a security cookie and acts as a "surrogate credential" accompanying each user request during a session. (Abstract, col. 3, lines 42-63).

Applicant respectfully submits that Kirsch and Luckenbaugh fail to teach or suggest

"determining by the second computer system whether the request represents a new transaction or an incomplete transaction by comparing a first value stored in the first computer system with a second value stored in the second system," as recited in claims 31, 41 and 51. In the present invention, the server (second system) compares a value stored in the client (first system) with a value stored in the server to *determine whether the user of the first computer system is attempting to establish a new transaction or to complete an incomplete transaction.* If the value in the client *matches* part of the value in the server, then the transaction is an incomplete transaction, as opposed to a new transaction.

In Kirsch, the cookie in the client computer system includes a coded identifier that corresponds to account information for the user of the client system, which is stored in the merchant server. When the user selects a purchasable product via the client system, the client system submits the selection with the cookie to the merchant server. The merchant server uses the cookie *to look-up the user's account record,* including billing related information, to fulfill the user's purchase request. (Col. 8, lines 14-20, col. 13, lines 32-34 (step 68, Figure 3)). Thus, contrary to the present invention, Kirsch uses the cookie to perform a look-up of a client user record, and fails to teach or suggest using the value in the client system to determine "whether the request represents a new transaction or an incomplete transaction," as recited in claims 31, 41 and 51.

In Luckenbaugh, when a user requests access to data stored in a server via a client system, the server uses the cookie *to look-up the user's identity and associated privileges*, which determines what the server returns to the user. (Col. 8, lines 53-61). Thus, contrary to the present invention, Luckenbaugh also fails to teach or suggest using the value in the client system to determine "whether the request represents a new transaction or an incomplete transaction," as recited in claims 31, 41 and 51.

Luckenbaugh does mention that a cookie can allow the "results of independent transactions which are part of the same user session to be associated with a larger session transaction," thereby "allowing an aggregate summation or totalization of the session transaction to be done." (Col. 5, lines 24-31). In other words, the cookie is associated with the session transaction and can be used to link or associate several independent transactions, e.g., places several purchases in a "virtual shopping cart," during a single session transaction. The session transaction terminates either when the web browser is terminated, i.e., the user session ends, or when the cookie expires. (Col. 5, lines 38-52). When the session transaction terminates, so does the cookie. Thus, the server determines whether a session transaction is an ongoing session or a new session by whether the client transmits a cookie or not. Accordingly, Applicant respectfully submits that Luckenbaugh's server does not determine "whether the request represents a new transaction or an incomplete transaction by *comparing*" the cookie transmitted by the client "with a second value" stored in the server, as recited in claims 31, 41 and 51.

Applicant respectfully submits that Kirsch and Luckenbaugh, alone or in combination, fail teach or suggest the present invention, as recited in claims 31, 41 and 51, and therefore that claims 31, 41 and 51 are allowable. Claims 32-40, 42-50, and 51-60 depend from claims 31, 41 and 51, and therefore the arguments above apply with equal force. Thus, Applicant respectfully submits that claims 32-40, 42-50, and 51-60 are also allowable over the cited references.

35 U.S.C. §103 Rejections

The Examiner rejected claims 6-10, 16-20, and 16-30 under 35 U.S.C. 103(a) as being unpatentable over Kirsch or Luckenbaugh in view of Graunke et al. (U.S. Patent No. 5,991,399). In so doing, the Examiner stated:

> **As per claims 6, 16, and 26, Kirsch discloses all the limitations of claims 5, 15, and 25, furth r;**

Graunke clearly teaches,
if the value in the co kie does n t match th value in the server system, step (c) further c mprises:

- **(c1) generating an encryption key;**
- **(c2) storing a portion of the encrypti n key in the co kie; and**
- **(c3) storing the entire encryption key on the server system (See Graunke abstract, figures 2, 4A and 4B and associated text, column 3, lines 5-20 and 60-68, column 6, lines 17-35, column 7, lines 8-68, and column 8, lines 1-31). . . .**

As per claims 9, 19, and 29, Kirsch discloses all the limitations of claims 5, 15, and 25, further;
Graunke clearly teaches, if the value in the cookie does match the value in the server system, ABC discloses that step (c) further comprises:

- **(c1) allowing the server system to transfer encrypted information to the client system; and**
- **(c2) allowing the server system to transfer a remaining portion of the encryption key to the client system whereby the encryption key is capable of being utilized by the client system to decrypt the encrypted information (see Graunke abstract, figures 2, 4A and 4B and associated text, column 3, lines 5-20 and 60-68, column 6, lines 17-35, column 7, lines 8-68, and column 8, lines 1-31).**

Applicant submits that claims 36, 46 and 56 are analogous to claims 6, 16 and 26, and that claims 39, 49 and 59 are analogous to claims 9, 19 and 29.

Applicant respectfully submits that claims 36-40, 46-50, and 56-60 depend on claims 31, 41 and 51, respectively, and the arguments regarding claims 31, 41 and 51 apply with equal force. As such, claims 36-40, 46-50, and 56-60 are allowable over the cited references.

Applicant also submits that claims 36-40, 46-50, and 56-60 are allowable for independent and additional reasons. For ease of reference, claims 36-40 are provided below.

> 36. The method of claim 31, wherein the request represents a new transaction if the first value does not match a part of the second value, the method further comprising:
> d) if the request represents a new transaction, generating a new encryption key by the second system, wherein the new encryption key is associated with the new transaction;
> e) storing a first portion of the new encryption key in the first computer system as the first value; and
> f) storing the whole new encryption key on the second computer system as the second value.
>
> 37. The method of claim 36 further comprising:
> g) encrypting the requested data with the whole new encryption key;
> h) transmitting the encrypted data from the second computer system to the first computer system; and

i) after the encrypted data has been transmitted, sending a remaining portion of the new encryption key from the second computer system to the first computer system,

wherein the first computer system combines the first portion and the remaining portion of the new encryption key to form the whole new encryption key and utilizes the whole new encryption key to decrypt the encrypted data.

38. The method of claim 37 further comprising:

j) after the encrypted data has been transmitted and prior to sending the remaining portion of the new encryption key, allowing the user to provide payment for the whole new encryption key.

39. The method of claim 31, wherein the first value is a first portion of an encryption key and the second value is a whole encryption key, and step c) further comprises:

c1) encrypting the requested data with the whole encryption key;

c2) transmitting the encrypted data from the second computer system to the first computer system; and

c3) after the encrypted data has been transmitted, sending a remaining portion of the encryption key from the second computer system to the first computer system, whereby the first computer system combines the first portion and the remaining portion of the encryption key to form the whole encryption key and utilizes the whole encryption key to decrypt the encrypted data.

40. The method of claim 39, wherein step (c) further comprises:

c4) after the encrypted data has been transmitted and prior to sending the remaining portion of the encryption key, allowing the user to provide payment for the whole encryption key.

Claims 46-50 and 56-60 are system and computer product claims having scopes similar to claims 36-40.

With regard to claims 36, 46 and 56, neither Kirsch nor Luckenbaugh in view of Graunke teach or suggest "generating a new encryption key by the second system" "if the first value does not match the a part of the second value." Graunke is directed to the "[s]ecure distribution of a private key to a user's application program (also called a 'trusted player' such as a DVD player or CD-ROM player) with conditional access based on verification of the trusted player's integrity and authenticity." (Abstract).

Graunke discloses "generating an asymmetric key pair . . . , encrypting predetermined

data with the generated public key, building an executable tamper resistant key module identified for the program, the executable tamper resistant key module including the generated private key and the encrypted predetermined data, and sending the executable tamper resistant key module to the remote system. The tamper resistant key module is then executed on the remote system to check the integrity and authenticity of the program and the integrity of the tamper resistant key module itself. If the validation process is successful, then the encrypted predetermined data is decrypted with the generated private key included in the tamper resistant key module." (Col. 3, lines 5-20).

Kirsch in combination with Graunke discloses a system whereby a client wishing to purchase digital content from a provider is authenticated via Kirsch's cookie and encryption keys for decrypting the digital content are securely transmitted to the client via Graunke's key module. Luckenbaugh in light of Graunke discloses a system that determines a user's privilege to access information in a server via Luckenbaugh's "security cookie," generates encryption keys and then securely transmits the encryption keys to the user via Graunke's key module.

In contrast to the present invention, the systems taught by the combination of Kirsch or Luckenbaugh and Graunke generate the key pair for encrypting the predetermined data either:

- after the data is *created* (Graunke, col. 8, lines 2-5; Figure 4A (step 102))
- after the program on the remote site requests the keys for decrypting the encrypted data (Graunke, col. 7, lines 16-30; Col. 8, lines 13-20; Figure 4A (step 106))
- after the client has been authenticated, i.e., cookie is valid (Kirsch, step 80 Figure 3, col. 13, lines) or
- after a user's credentials have been determined (Luckenbaugh, col. 8, lines 53-65).

None of the above instances teaches or suggests "generating a new encryption key" "if the first value *does not* match a part of the second value," as recited in claims 36, 46 and 56.

Accordingly, Applicant respectfully submits that claims 36, 46 and 56 are allowable over the cited references.

Moreover, none of the references teaches or suggests "storing a first portion of the new encryption key in the first computer system as the first value," as recited in claims 36, 46 and 56. In contrast to the present invention, Graunke stores the key pair for decrypting the encrypted data in the server database (col. 8, lines 2-5), and includes the key pair in the key module (col. 7, lines 53-55). The key module also includes "an asymmetric public key for verifying the digital signature of the manifest . . . . and an asymmetric private key for decrypting the encrypted symmetric public keys when the validity of the trusted player on the client is assured." (Col. 7, lines 46-57). The key module does not include *a first portion* of a key. Nothing in Kirsch or Luckenbaugh in view of Graunke teaches or suggests "storing a first *portion* of the new encryption key in the first computer system as the first value," as recited in claims 36, 46 and 56.

In the Office Action, the Examiner indicates that "there has been no clear understanding of the term 'a portion of ...' and clarification of such has not been found within the specification. Therefore, it was interpreted that the 'a portion of ...' could be the all of the encryption key." Applicant respectfully disagrees.

First, as stated above, the clear definition of the term "portion" is "a part or share" of a larger entity. Thus, interpreting "a first portion of a new encryption key" as an entire encryption key clearly defies the ordinary and common definition of the word "portion." Secondly, the Specification makes clear that when a request represents a new transaction, i.e., when the first value does not match the second value, the server generates an encryption or session key, and "instructs the browser [on the client] to create a cookie on the client system and store half (the high 128 bits) of the session key in the cookie." Specification, page 5, lines 5-12. Half of the encryption key is a "portion" of the entire encryption key.

Because Kirsch or Luckenbaugh in view of Graunke fails to teach or suggest "generating a new encryption key," and "storing *a first portion* of the new encryption key in the first computer system as the first value" "*if* the first value *does not* match the second value," as recited in claims 36, 46 and 56, claims 36, 46 and 56 are allowable.

As for claims 37, 39, 47, 49, 57 and 59, Applicant respectfully submits that Kirsch or Luckenbaugh in view of Graunke fails to teach or suggest "sending *a remaining portion*" of the encryption key to the first computer system, "wherein the first computer system combines the first portion and the remaining portion" of the encryption key to form the whole encryption key. As stated above, Graunke's key module *does not* include *a portion* of an encryption key. All of the keys in the key module are complete public or private keys. Accordingly, Applicant respectfully submits that claims 37, 39, 47, 49, 57 and 59 are allowable over the cited references.

Claims 38, 40, 48, 50, 58 and 60 depend on claims 37, 39, 47, 49, 57 and 59, respectively, and therefore the above arguments apply with equal force. Thus, claims 38, 40, 48, 50, 58 and 60 are also allowable over the cited references.

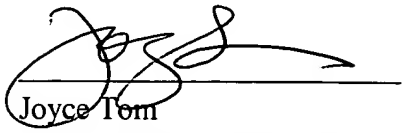
Conclusion

In view of the foregoing, it is submitted that the claims 31-60 are allowable over the cited references and are in condition for allowance. Applicant respectfully requests reconsideration of the rejections and objections to the claims, as now presented.

Applicant believes that this application is in condition for allowance. Should any unresolved issues remain, Examiner is invited to call Applicants' attorney at the telephone number indicated below.

Respectfully submitted,
SAWYER LAW GROUP LLP

May 10, 2004
Date



Joyce Tom
Attorneys for Applicant(s)
Reg. No. 48,681
(650) 493-4540